

REMARKS

I. INTRODUCTION

Claims 1, 10, 16, and 19 have been amended, and thus remains pending in the present application. In view of the above amendments and the following remarks, it is respectfully submitted that all of the presently pending claims are allowable.

II. THE 35 U.S.C. § 103(a) REJECTION SHOULD BE WITHDRAWN

The Examiner has rejected claims 1-3, 6, 10, 11, and 15-18 under 35 U.S.C. § 103(a) as obvious over U.S. Pat. No. 6,760,444 ("Leung") in view of U.S. Pat. No. 5,732,350 ("Marko"). (See 05/31/07 Office Action, p. 5).

Claim 1 has been amended as follows:

A method for authenticating a roaming device with a network, comprising the steps of:
generating, by an authentication server of the network, authentication data associated with the roaming device;
sending the authentication data to access points of the network, the access points being connected to the authentication server; and
when the roaming device roams to a particular access point of the access points, determining if the particular access point has authentication data associated with the roaming device, using the authentication data to locally authenticate the roaming device at the particular access point if the determination is positive, or carrying out the authentication process at the authentication server if the determination is negative.

Support for the amendment is found at least at paragraphs [0013]-[0018] of the Specification. Leung discloses a method for authenticating a roaming device with a network,

comprising the steps of generating by an authentication server of the network, authentication data associated with the roaming device, sending the authentication data to a Home Agent of the network which is connected to the authentication server, and using the authentication data to locally authenticate the roaming device at the particular access point. (See Leung Abstract).

Marko discloses a method for registering a mobile station among a plurality of base stations defined by a cell grouping level based upon a dynamic algorithm, when the base station registers with an initial base station and the base station provides a cell grouping level. (See Marko Abstract).

The Examiner stated that because Leung teaches the steps of generating, sending and using the authentication data to locally authenticate the roaming device with a network, and because Marko teaches the method for registering a mobile station with multiple base stations, thus the combination of these two covers the limitations of claim 1. But neither Leung nor Marko teaches the newly amended claim 1 because neither teaches the step of “determining if the particular access point has authentication data associated with the roaming device, *using the authentication data to locally authenticate the roaming device at the particular access point if the determination is positive, or carrying out the authentication process at the authentication server if the determination is negative.*”

In the claimed invention, the access point, upon being contacted by a mobile station, first determines whether a WEP-session key has already been generated for the mobile station by the authentication server and been broadcasted to the access points within the ESS, and then the authentication process will diverge based on the determination result. (See Specification [0018]-[0023]). If a WEP-session key associated with the mobile station has already been generated and stored in the access point, the access point will start to perform the authentication process locally. (See Specification [0021], [0022]). On the other hand, if the WEP-session key has not been generated, the authentication process will take place in the authentication server, then the WEP key will be sent to the current access point connected to the mobile station and also the additional access points in the ESS. (See Specification [0018]).

However, it is clear that the system in Leung does not perform the above-mentioned step to determine where the authentication procedure will take place. Specifically, the authentication of the mobile node in Leung can be performed either by the server which provides a plurality of security associations for a plurality of mobile nodes, or by the Home Agent locally. (See Leung Abstract, Fig. 7, Fig. 8). Nevertheless, where to perform the authentication is not triggered by any particular condition, such as the Home Agent's determining if it has the authentication data associated with the mobile node, but is configured according to the preference of the network operator. (See Leung col. 8, line 13-25). Indeed, the Home Agent in both these two embodiments of the devices only checks the mobile node list stored on the Home Agent to identify which authentication server handles security associations for the particular mobile node making the registration request, then sends out different packet data to the server based on the operational preference. (See Fig. 7, Fig. 8, col. 7, line 10-30, col. 8, line 30-50).

Accordingly, it is respectfully submitted that neither Leung nor Marko nor the combination of them teaches claim 1 because neither teaches the step of "determining if the particular access point has authentication data associated with the roaming device, using the authentication data to locally authenticate the roaming device at the particular access point if the determination is positive, or carrying out the authentication process at the authentication server if the determination is negative." Accordingly, it is respectfully submitted that claims 1-3, 6, 10-11, and 15-18 are therefore allowable.

Claims 4 and 5 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leung in view of Marko and in further view of U.S. Pat. No. 5,408,683 to Ablay et al. ("Ablay"). (See Office Action, pp. 11-12). However the further combination of Ablay does not cure the above-mentioned deficiency of Leung and Marko. Thus, it is respectfully submitted that claims 4 and 5 which depend from and, therefore, include all of the limitations of claim 1 are also allowable.

Claims 7, 8, and 13 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leung in view of Marko and in further view of U.S. Pat. No. 6,452,910 to Vij et al. ("Vij"). (See Office Action, pp. 12-14). However the further combination of Vij does not cure the above-mentioned deficiency of Leung and Marko. Thus, it is respectfully submitted that claims 7, 8,

and 13 which depend from and, therefore, include all of the limitations of claim 1 and 10 are also allowable.

Claims 9, 12, and 14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leung in view of Marko and in further view of U.S. Pat. Pub. No. 2002/0174335 to Zhang ("Zhang"). (See Office Action, pp. 14-16). However the further combination of Zhang does not cure the above-mentioned deficiency of Leung and Marko. Thus, it is respectfully submitted that claims 9, 12, and 14 which depend from and, therefore, include all of the limitations of claim 1 and 10 are also allowable.

Claim 19 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Leung in view of Zhang, with RFC 2138 incorporated to illustrate inherent properties of the RADIUS protocol. (See Office Action, pp. 16-18).

Zhang is directed toward converging both the authentication, accounting, and authorization process with data transmissions at the Internet Protocol layer. (See Zhang, Abstract). Zhang still maintains a communication with the access point to an authentication server to authenticate mobile devices. (See *Id.*, [0074]–[0078]).

Claim 19 recites as follows:

A method for authenticating a roaming device with a network, comprising the steps of:

with an authentication server, receiving an authentication request from a roaming device if the access point connected with the roaming device has no authentication data associated with the roaming device, the request being encrypted with a first shared code;

with the authentication server, generating a session key associated with the roaming device;

sending the session key to an access point of the network, the session key being encrypted with a second shared code; and

utilizing the session key to authenticate the roaming device at the access point, and to encrypt data exchanged between the roaming device and the access point.

It is respectfully submitted that neither Zhang nor the combination of Zhang and Leung teaches that "an authentication server, receiving an authentication request from a roaming device *if the access point connected with the roaming device has no authentication data associated with the roaming device.*" Leung has been discussed above. In contrast with the claimed invention, Zhang does not suggest such an authentication server. In particular, the Examiner does not state how Leung shows that its purported authentication server receives the request "if the access point... has not authentication data...." Because of this absence, the Examiner has not established a prima facie case of obviousness. Thus, it is respectfully submitted that one skilled in the art would not find the combination of Leung in view of Zhang obvious over claim 19. Accordingly, it is respectfully submitted that claim 19 is therefore allowable.

Claim 20 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Leung in view of Zhang and in further view of Marko. (See Office Action, pp. 18-19). Leung, Zhang, and Marko have been discussed. The combination of the three references does not cure the deficiency mentioned above regarding claim 19. Thus, it is respectfully submitted that claim 20 which depends from and, therefore, includes all of the limitations of claim 19 is also allowable.

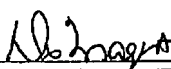
Claim 21 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Leung in view of Zhang and in further view of U.S. Pat. No. 6,178,506 to Quick, Jr. ("Quick"). (See Office Action, pp. 19-20). Leung, Zhang, and Marko have been discussed. The combination of the three references does not cure the deficiency mentioned above regarding claim 19. Thus, it is respectfully submitted that claim 21 which depends from and, therefore, includes all of the limitations of claim 19 is also allowable.

CONCLUSION

In view of the above remarks, it is respectfully submitted that all the presently pending claims are in condition for allowance. All issues raised by the Examiner having been addressed, an early and favorable action on the merits is earnestly solicited.

Respectfully submitted,

Dated: August 31, 2007

By: 
Dervis Magistrate (Reg. No. 41,172)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, New York 10038
Tel: (212) 619-6000
Fax: (212) 619-0276